Netherlands organization for applied scientific research

TNO-report

TNO Physics and Electronics Laboratory

P.O. Box 96 TD
2509 JG The Hague
Oude Waalsdorperweg 63
The Hague The Netherlands

Fax +31 70 328 09 61
Phone +31 70 326 42 21

report no. FEL-91-B100

copy no. 8

(1)

title

Information Security: Past, Present and Future

author(s):

P.L. Overbeek

date :

March 1991

classification	
title	: unclassified
abstract	: unclassified
report text	: unclassified
appendix A	: unclassified

no. of copies	: 25
no. of pages	: 42 (incl. appendix, excl. RDP & distribution list)
appendices	: 1

All information which is classified according to Dutch regulations shall be treated by the recipient in the same way as classified information of corresponding value in his own country. No part of this information will be disclosed to any party.

TNO

report no.	:	FEL-91-B100
title	:	Information Security: Past, Present and Future
author(s)	:	P.L. Overbeek
institute	:	TNO Physics and Electronics Laboratory
date	:	March 1991
NDRO no.	:	
no. in pow '91	:	709.2
Research supervised by:		D.W. Fikkert, H.A.M. Luijf
Research carried out by:		P.L. Overbeek

ABSTRACT (unclassified)

The development of information security is addressed in relation to the development of information technology. The leading question is: how has information security developed itself so far, and how should it progress to address tomorrow's security needs.
This study has been performed as part of the PhD-project SEDIS (Securable Distributed Information Systems). This project aims at a better understanding of and contribution to security in distributed information systems.
This paper has been presented at Securicom '91, "9e Congrès Mondial de la Protection et de la Sécurité Informatique et des Communications".

rapport no.	:	FEL-91-B100
titel	:	Information Security: Past, Present and Future
auteur(s)	:	ir. P.L. Overbeek
instituut	:	Fysisch en Elektronisch Laboratorium TNO
datum	:	maart 1991
hdo-opdr.no.	:	
no. in iwp '91	:	709.2
Onderzoek uitgevoerd o.l.v.	:	D.W. Fikkert, ir. H.A.M. Luijf
Onderzoek uitgevoerd door	:	ir. P.L. Overbeek

SAMENVATTING (ongerubriceerd)

De ontwikkeling van informatiebeveiliging wordt besproken in relatie tot de ontwikkelingen in de informatie technologie. De vraag is: hoe heeft informatiebeveiliging zich tot nu toe ontwikkeld, en in welke richting zou deze ontwikkeling verder moeten gaan om in de toekomst aan de zich veranderende beveiligingsbehoeften te voldoen.
Dit onderzoek is uitgevoerd als onderdeel van het promotieonderzoek SEDIS (Securable *Distributed Information Systems). Dit project beoogt inzicht te verwerven in, en bij te dragen aan* beveiliging in gedistribueerde informatie systemen.
Deze studie is gepresenteerd op Securicom '91, "9e Congrès Mondial de la Protection et de la Sécurité Informatique et des Communications".

CONTENTS

1. INTRODUCTION

In this paper the development of information security is addressed in relation to the development of information technology (IT). The main topic is: how has information security developed itself so far, and where should it go in order to address the security needs of tomorrow.

First some terms and definitions are presented. Next an overview is given of information technology in the past and present in relation to the security needs and requirements, the solutions and remaining problems in each period. From this overview of past and present, future developments in IT are discussed as well as the security requirements that must be fulfilled to achieve an acceptable level of security in future systems.

It will no longer be acceptable to develop new IT-products first and add in security afterwards. Security must be a major design criterion for tomorrow's IT-products. If information security does not keep up with the developments in information technology, the practical use of new technologies will be seriously hindered, if not stopped.

2. PROFESSIONAL LANGUAGE

In the area of information security no general accepted set of terms and definitions exists. For this reason a short definition of terms as used in this paper is given. First the qualities of information are discussed, next the security measures and finally the effect of measures.

2.1 The Value of Information: What are the Qualities of Information?

The purpose of information security is the safety of information. *Safety* is the absence of risks that are not wittingly accepted. *Security* is the means to achieve safety. The value of information needs to be secured. This value is determined by the following qualities:

1 *Confidentiality* is the privacy and exclusive use of information.
2 *Integrity* is the correctness and completeness of the information as well as the information being up-to-date.
3 *Availability* is the ability to have access to services and information within a certain time frame.

Information security in itself is not a goal. Information security must support the objectives of an organisation. Thus, the security measures must reflect the needs within the organisation. Not all information is equally valuable. This value of the information must be taken into account when security measures are selected.

2.2 Security Measures

By applying security measures, risks that threaten the qualities of information can be reduced or excluded. Starting point and most important is a good *organisation* of security, with clearly defined responsibilities and duties, guidelines, management reports and coordination between the various security measures. *Physical* security measures, like the isolation of the computer room, are relatively simple to take and can be very effective. *Technical* security measures offer security within a system (application, operating system or network). This is for example the security offered by an operating system, taking care of separation of users and data, and the access control to the system. *Procedural* security defines what actions must be taken by the employees in specific situations. Procedures must, for example, define who has access to the computer room; define the expiration of an account and the handling of the remaining information.

Security measures are only effective when all measures are balanced. This tuning of the security measures must be taken care of in the organisation of security.

2.3 Effect of Security Measures

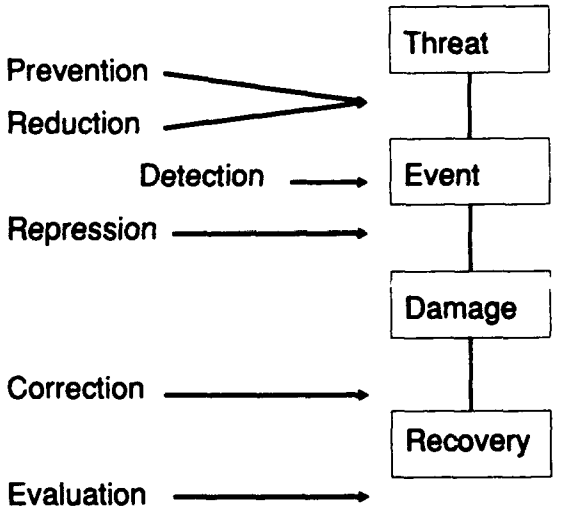


Figure 1: Event cycle

Security measures have their effect at a specific moment in the event cycle, see figure 1. At the top of the event cycle is the threat that security might be breached. Should this happen it is called a security event. This event causes damage as loss of information or services that must be recovered.

All these steps need to be addressed when security measures are planned.

Specific security measures can be applied to each step. First, of course, the occurrence of an event must be excluded or prevented by *preventive* measures. At the same time, the possible loss resulting from an anticipated event can be minimised by *reductive* measures. When an event has

occurred, it must be discovered as soon as possible. This is done by *detective* measures. *Repressive* measures stop the continuation or reoccurrence of an event, thus reducing losses. Next, the information and services are restored as good as possible by *corrective* measures. In some cases, this is the beginning of an uncertain period in which integrity and confidentiality might be breached.

In case of a serious event, it is worthwhile to *evaluate* the event: what went wrong, how did it happen and which measures should be taken. Beside this evaluation on a per-event basis, it is helpful to have an organisation-wide overview of security events. This can easily be achieved by means of a reporting procedure for security events. This overview assists in the evaluation of the effectiveness of the current security measures and is input for the preparation of a new security plan.

3. DEVELOPMENT OF INFORMATION TECHNOLOGY AND INFORMATION SECURITY

In this section, it is shown how information technology has developed from the classic computer with card reader to the current situation of cooperating but independent computer systems in networks. Also foreseeable trends in the use of IT and future developments are discussed. Together with the IT-developments, the evolution of information security is discussed. For this purpose, we regard per period:

- the security needs (confidentiality, integrity and availability);
- the relative importance of physical, technical, and procedural security;
- the assignment of responsibilities for security as an important example of organisational security;
- the most commonly used security measures.

This overview intends to illustrate the changes in security during the course of IT-developments; there is no pretending of completeness.

3.1 Past

The modern history of information technology has been written in the past three decades. In the early days of commercial use of IT, most of the processing was batch oriented followed by the rise of interactive processing.

3.1.1 Batch Period

3.1.1.1 IT Environment

When computations in the sixties started to be performed on computers, programs were written in a language which was close to 'the machine', like assembly language. The machine was being fed with punched cards and the result of a job was a printout. Computing was batch oriented.
The card reader was used to queue the jobs. The operating system just took the next job (a desk of cards) from the queue when the previous job had finished. At one time, there was only one job in the system. Because of this straightforward operation, the operating system was relatively simple. Later on, batch processing was enhanced by multiprogramming. More jobs could be simultaneously in the system, one job active, the other jobs waiting.

3.1.1.2 Security

The computer had to be protected because it was expensive and vulnerable for changes in the environment (humidity, temperature, shocks) and human errors. Therefore, the computer was physically secured in a room with environmental control and restricted access. Input (punched cards) and output (printouts, listings) took place by means of a counter at the central computer room. In addition the employees at the counter performed some kind of a (social) check on computer use.
Job Control Language (JCL) was used to create access to the right disks and data sets. Access control was often done before the actual job was started and was based on the information on the JCL account card, if done at all. This control aimed at preventing unauthorised access to complete data sets (files), merely to protect confidentiality. Integrity was not a major issue, since the results of a job were redirected to the user who kept the responsibility for checking the proper execution of his job. Availability too was not very important. The machine went down regularly and the turn-around time for a job was a matter of hours or days.

The responsibility for maintaining the proper security measures to secure the information and the hardware at the central site was assigned to the head of the computer centre by the users (being the owners of the information). The users remained responsible for the security of account information and the desks of punched cards in their possession.
Security was merely physical, supported by procedures. Technical security was limited to preventive measures based on the information on the account card.

3.1.2 Interactive Period

3.1.2.1 IT Environment

For certain tasks like the management of the system itself, batch processing was not practical. In the seventies, interactive processing solved many of the problems. In interactive processing an interrupt mechanism is used in stead of a queue mechanism.
One of the applications of interactive processing was the substitution of the punched cards by electronic equivalents: card-images could be created, changed and stored from a terminal. The job, an electronic pile of cards, was still served as a batch process.
The user no longer physically had to go to the counter of the system and did not use punched cards any more. He typed his commands, programs and information in at a terminal connected to the system.

Not all manufacturers took the step towards interactive processing in the same manner. Others had a different background, e.g. in real time processing.

Operating systems became more complex. In an interactive environment several jobs are competing for resources and processing time. The operating system is responsible for a fair allocation of scarce resources and processing time to the jobs in time.

Interactive processing does not replace batch processing. Working in an interactive way provides the user for other information needs than batch processing.

3.1.2.2 Security

The rise of interactive processing brought new security problems: the anonymous users at the terminals had to be authenticated; the communications between terminal and computer system was insecure; the users in the system had to be separated from one another, each other's data and the operating system.
Because of the co-location of the computer, printer and disks at the central computer room, physical security still was effective. Technical security had to be improved because of the different security needs in an interactive environment. So far, security in information systems (applications, operating systems and communications) never was a real design issue. Security had to be 'glued in' afterwards. However, it is quite difficult to create a secure product starting from an insecure product, since all of the security holes in the product must be found and repaired. Even if this 'exercise in paranoia' proved to be successful, this operation caused decrease in performance and functionality. It also gave security a bad public image: there are still people that regard security as something that is limiting possibilities instead of offering additional functionality.

Technical Security

Technical security became more important. The most important concept for the realisation of technical security is the concept of the reference monitor (figure 2), also known from the 'Orange Book' [1].

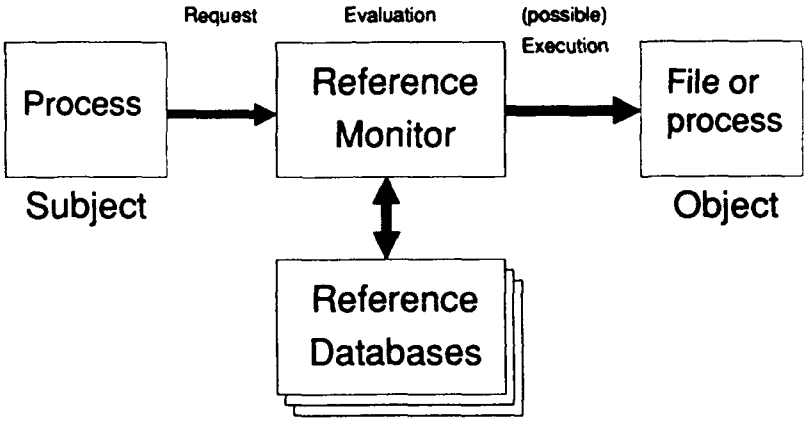


Figure 2: The Reference Monitor

The idea behind the reference monitor is simple: every request for a security-relevant action in the system is evaluated before the (possible) execution. The initiating entity of a request is called the *subject*, the addressed entity is called the *object*. The reference monitor guarantees controlled state transitions from a safe situation to another safe state.

The evaluation is based on static security information (rights of the user or process; requirements for the access of a certain file or other process) and dynamic security information (other processes working on the same object; specific system management taking place; time of day; history).

The security information is available in security reference databases. Changes to this security information are also under the control of the reference monitor. The reference monitor is responsible both for the decision and the enforcement of that decision.

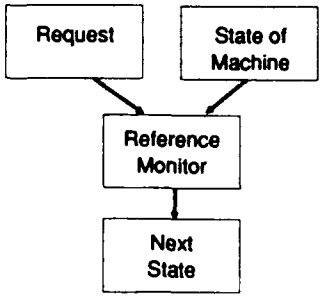


Figure 3: Single-State Machine

The set of entities in the system under control of one reference monitor is called the *domain*. An entity is controlled by one reference monitor. During an evaluation, no security relevant changes in the system that are inside the domain of the reference monitor are possible. The situation is frozen, thus creating a single-state machine (figure 3).

The main characteristics of the reference monitor can be summarised as follows:

1 The reference monitor creates a single-state machine that allows only transitions from one secure state to another.
2 The reference mor[illegible] mediates all changes within his domain. During the evaluation of a request the situation in the domain is frozen.
3 The security information that is needed by the reference monitor is under its control, including changes to this information.

Other Security Issues

Still, the responsibility for the security measures at the central site was properly assigned by the users to the head of the computer centre. It was not too difficult to take care of the enlarged technical security, as part of the daily operations. The users got more responsibilities, e.g. for the use of accounts and their rights in the system.

Physical security remained effective since all the valuable information was centrally stored.

Procedural security, carried out mostly by employees at the computer centre and partly by the users, became more complex.

Security still concentrated on prevention; additionally, reduction and detection (audit) were introduced.

The necessity of information security was often not properly recognised, as the population of users was more or less known and assumed to be trustworthy.

3.2 Present: a Multi-Vendor Environment with Networks of Independent Systems

3.2.1 IT Environment

In the eighties, the number of computer systems in an organisation increases rapidly. To exchange information between computer systems, computer networks are installed. Today, these computer networks are used for terminal access as well. The user is no longer working with a dumb terminal but with a PC or workstation being part of a network. An average IT environment includes systems from several vendors and different operating systems. The network connects mainframes, mini's, servers, workstations and PC's. Part of this infrastructure is still located at the central computer room and managed by the computer centre. Another part is being managed by the users themselves and lies outside the control of the central organisation. The connectivity between systems is achieved by multiple network protocols sometimes multiplexed over the same cables.

Local area networks (networks on one location and owned by the organisation at that location) are connected to wide area networks (networks between locations and using the public infrastructure owned by a service provider, e.g. PTT). This public infrastructure is also accessible for remote services.

A rising phenomenon is the diminishing difference between local processing and distributed processing in the network. The actual locations of storage and processing are assigned dynamically.

At the same time and somewhat contradictory, these new technological opportunities do not bring us any closer to truly reliable information systems in which information is safely processed and stored. Complex information systems must operate in an IT environment that is continuously changing. The behaviour if these systems cannot be predicted in advance. It is on this challenging environment, that many social demands and business assets are depending.

Summarising: networks become more important because of the rise of low-cost workstations and PC's. Gradually, a separation is emerging between the actual location of storage media (on file servers) and the actual location where processing takes place (on a PC, workstation or a special server). Networks are vital for the necessary connectivity and services.

3.2.2 Security

The challenge now and for the future is that information security must fit in a multi-vendor environment with different operating systems and networks using different protocols. We must assume that the IT infrastructure is shared with unreliable and unpredictable participants (computer systems, networks, users, software). Connectivity is a must. The information flow is not restricted to one specific computer system, operating system or network, or not even to a specific application. Information security must be able to secure the information all the way, and therefore the information flow (and thus, the connectivity). To achieve this in a multi-vendor situation, standardisation is essential [4]. The most important organisations in the arena of standardisation are ISO, ECMA and CCITT [3, 7, 8]. The process of security standardisation evolves thoroughly, but slowly [9].

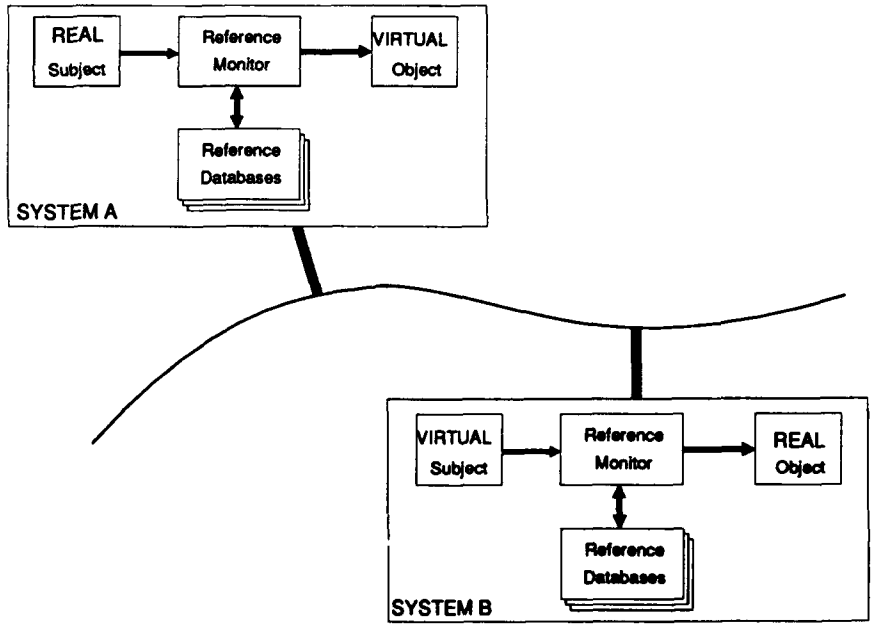


Figure 4: Two Reference Monitors in a Network

3.2.2.1 Technical Security

Today, information security is 'host'-oriented. This means that the security is organised per computer system. The technical security per host is based on the concept of the reference monitor, as we have seen above.

Is this concept still suitable when information flows from one system to another in the network? In figure 4 the situation of two cooperating reference monitors on systems A and B in a network is represented. The question is if these reference monitors together are able to offer the same functionality as one.

In the case that a subject at system A is asking for access to an object at system B, these two reference monitors must exchange information. The request must be evaluated by both monitors. Now, these reference monitors must be able to trust each others authenticity, functionality and each others information. How to achieve this in an insecure network, shared by untrustworthy systems? Are the main characteristics of the reference monitor still met?

1 There is no single state in the network, since there are more systems and more reference monitors working independently of each other.
2 Therefore, the network is not a single domain with one reference monitor that mediates all changes.
3 The security information that is needed by the reference monitor is no longer strictly under its own control, nor are any changes to this information.

The conclusion is that this solution is not unquestionable. We may be absolutely confident that the network is not being attacked and the communicating systems are both authentic and are implementing the same security policy (i.e. managed in the same way). Yet, the cooperating reference monitors do not provide a single state.

When seen from a security point of view, the systems in a network are isles that might be secure, within the insecure network. If two secure systems are interconnected it does not result in a new secure system, not at all if insecure means are used [2].

3.2.2.2 Responsibilities

How are responsibilities for information security assigned today? It is not likely that these assignments are still the same as they were in the batch period. The tendency is towards distributed processing in networks using PC's and workstations. The involvement of the computer centre with microcomputers is often minor. For security, the absence of a central organisation for security can have disadvantages:

1 In the past, the users (being the owners of the information) delegated many of the responsibilities for information security to the head of the computer centre. However, in a distributed environment some of the responsibilities for information security shift back towards the users. The unattractive situation arises of an unclear division of responsibilities between the users and the computer centre. It must be avoided that parts of the IT infrastructure or information bases emerge for which nobody feels responsible. Some examples:

   Example 1: Users are responsible for the security of the information on 'their' PC in the network. Do they have the means to do this properly?

   Example 2: The PTT's do not accept responsibility for the security of information that is transported through the public infrastructure. Then who is responsible, users or computer centre?

   Example 3: Local area networks are easy to tap. Which security services should or may be expected from those who are responsible for security in a local area network?

2 Working in an environment with workstations and PC's in networks enlarges the need for security. Firstly, this is because of the fact that networks bring some inevitable security problems. Secondly, the number of systems that need to be secured is growing.
   It must be mentioned here that networks also bring many good points from the viewpoint of security. Networks re-enable the possibility to offer central (security) services and management for users at decentralised workstations and PC's.

At many computer centres the priorities remain with the central systems. The computer centre should ask itself whether the situation above exists, and if so, how their security activities should be extended. At a higher management level, having seen the changes in the use of IT, the assignment of responsibilities must be re-evaluated. This may include organisational changes.

3.2.2.3 Management and Automated Tools for Security

The employees that are responsible for technical security do not have an easy job. The necessary consistency between application, system, and network security cannot be derived with today's means. There is a lack of automated tools for information security, especially in a network environment. The available tools are primarily focussing on prevention, leaving the needs for the other security measures of the event cycle almost unanswered.

Integrity control, both for information and software, is still a research topic. The need for a more comprehensive approach to availability of services and information is not even recognised by an organisation like the ISO [3, 6, 8].

3.2.2.4 Procedural Security

The effectiveness of procedures drops when an increasing number of people are supposed to conform to them. It does make a difference whether one person is responsible for making the back-up of all the data or that many people carry out part of it. Many investigations in this area mention that most of the security events are caused by own employees [5, 10]. The awareness of the employees is said to be of major importance. Proper training and a regular check on the employees can be helpful, working both preventive and detective. However, this never will solve the entire problem.

The question arises if this dependency on the good will of one's own employees is favourable. Is it not true that information systems have become too vulnerable for human failures? Technology must provide solutions for this problem.

3.2.2.5 Physical Security

In the past, only one central computer room needed protection to secure the information. Today, information is stored and processed at many places. The security of all parts of the IT infrastructure must be balanced. It is, for example, not useful to fortify your PC if you are using a nearly open network for the same information.

3.3 Future

3.3.1 IT Environment

A number of trends are recognised.

1 Networks will become even more important in the future. The same increase in the use of local area networks will be seen in the area of wide area networks. More and more networks will be connected. Services and wide area networks will be in shared use by different organisations.

2 The user will no longer be tied to one working place. At every PC or workstation, in- or outside his organisation, he will be able to perform his duties. The equipment to do this will be highly portable (this trend is more or less equivalent to the current development of the personal telephone).

3 The user will no longer experience a difference between local and remote processing or storage. Tasks are executed where the resources happen to be available. Information services will be distributed, including processing and storage.

To achieve this, further standardisation of network protocols is needed. Furthermore, (different) operating systems must be adapted to distribution in a network, for example, to be informed about available resources and services in other systems.

3.3.2 Security

Today, some services for information exchange between different organisations are available already, although not yet commonly used. If these services are not secured then only information with low security demands can be processed and organisations will not be able to use these services for all their business purposes (an example of this is the current use of electronic mail for information exchange between organisations). The lack of security will seriously hinder the commercial development of services in the future.

To withstand the new security problems in a situation in which IT is no longer organised around the computer system but around the network, and taking into account the growing needs for information security, solutions must be found in the following areas:

1 Technical security in applications, operating systems and networks must be improved and integrated. Today, a computer system has no means to get information about security services in the network and about other systems. The same holds for applications [9]. Security of information flow, storage, and processing can only be achieved when security information can be exchanged. The format of the security information and the exchange of it must be standardised.
It must be avoided that each application has to be secured individually. We must strive towards general security solutions.

2 Future systems must be able to address integrity of information and software.

3 Availability of services and accessibility of information will be major security issues. This includes not only the protection against disruptions, but also the provision of alternative routing and distribution in order to maintain access to information and services. This is achievable in a distributed environment since the same information can be reached using various connections and perhaps, using redundant storage, even at multiple locations. Also, the same services can be provided at more systems.

4 Information will be transported more often via possibly hostile networks and stored in possibly insecure computer systems. The protection of information can be based on cryptography. Cryptographic techniques must bind together owner and information, and should be independent of the possible destination. Although these techniques are available, the use of cryptography is not yet widespread.

5 Preventive security measures remain of importance. Measures for detection, repression and correction will become equally important.

6 The management of complex information systems including security management needs special attention.

4. CONCLUSIONS

It has been made clear that the developments in information technology have consequences for security. It has been shown that this implies changes in the organisational security (assignment of responsibilities), an increasing impact of technical security, and a decreasing effectiveness of physical and procedural security.
Security has stayed behind compared to the developments in information technology, especially were the use of networks is considered. It has been shown that the concept of the reference monitor, which is host-oriented, is not very suitable in network situations.
To prevent that technical security will remain an underdeveloped area, solutions are to be found in the following areas:

- Distribution of security in networks;
- Integration of application, operating system and network security;
- Mechanisms that fulfil the needs for availability and integrity;
- Security measures for detection, repression and correction;
- Standardisation (which is essential for security between systems from different vendors).

It has been shown that changes in organisational security will take place because of the shifts in responsibilities. This will also effect the management of distributed systems.

If information security does not keep up with the developments in information technology, the practical use of the new technology will be seriously hindered, if not stopped.

5. REFERENCES

[1] Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28 STD.

[2] Information Technology Security Evaluation Criteria (ITSEC), Draft May 1990.

[3] ISO 7498-2, Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Security Architecture

[4] In: T.A. Berson, T.Beth (Eds), "Local Area Network Security", proceedings Workshop LANSEC 1989, ISBN 3-540-51754

[5] JJ Buch BloomBecker, "Trends in Computer Abuse/Misuse; in: "Information Systems Security", proceedings NIST/NCSC 12th National Computer Security Conference (1989)

[6] "Working Draft Access Control Framework", ISO/IEC JTC1/SC21 N5045

[7] "Guide to Open System Security", ISO/IEC JTC 1/SC21 N5049

[8] "Taxonomy for Security Standardisation", CEN/CENELEC Security Group, CSecG/49/90 (ISO/IEC JTC 1 N1040)

[9] P. Overbeek, "OSI Security and Relations with other Security Standards", in: Shape Technical Centre, Proceedings OSI Symposium 1990, SP-8 volume 2.

[10] In: "Computer Security and Information Integrity in Our Changing World", proceedings 6th IFIP TC-11 conference, May 1990.

D.W. Fikkert
(projectleader)

Ir. H.A.M. Luijf
(supervisor)

Ir. P.L. Overbeek
(author)

PRESENTATION SHEETS

Deze bijlage bevat 18 sheets.

This appendix contains 18 sheets.

Information security: past, present and future
Impact of Developments in IT on security

Paul Overbeek
TNO Physics and Electronics Laboratory
The Netherlands

Information Security
Networks

SEDIS

Information Security must
anticipate on changes in IT

Securicom '91

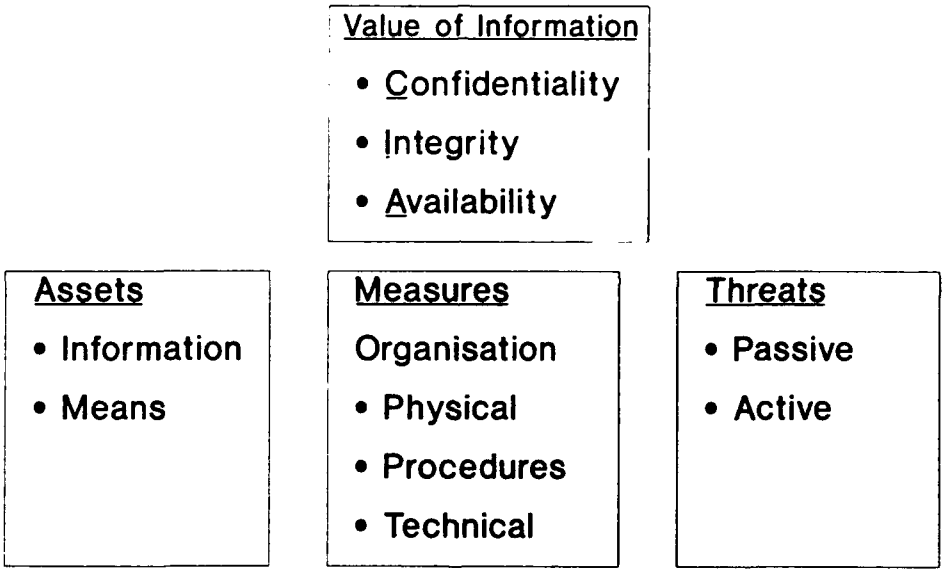
Information security: past, present and future
Impact of Developments in IT on security

Contents:

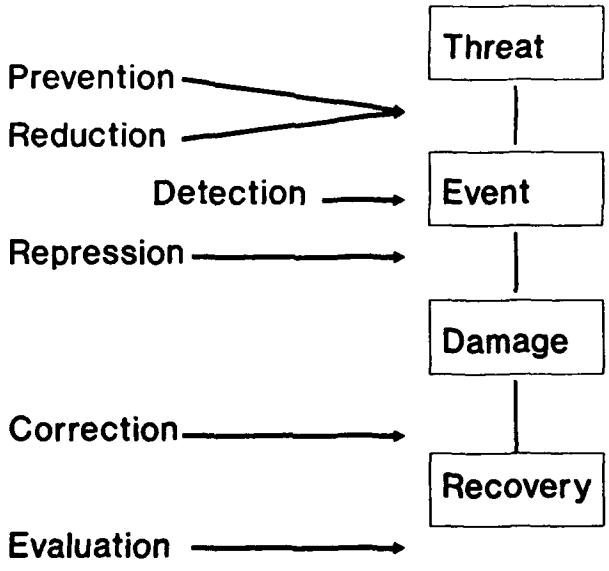
- A Professional Language
- Development of IT and Information Security
  - Past
  - Present
  - Future
- Implications for
  - security organisation
  - procedures
  - physical security
  - technical security
- Where to go now?

Securicom '91

Professional Language



Event Cycle


Threat
Prevention
Reduction
Event
Detection
Repression
Damage
Correction
Recovery
Evaluation

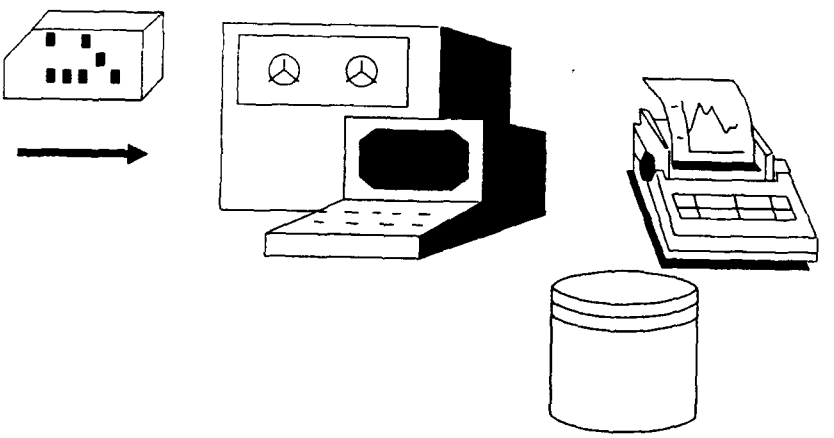
Development of IT and Information Security Past, Present and Future

Per period:

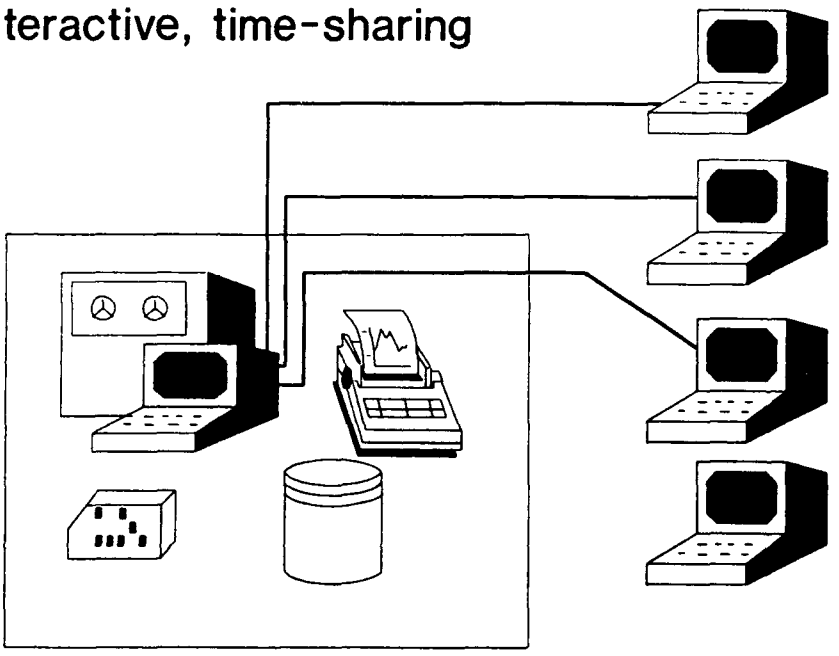
- Typical IT-environment
- Security Needs
- Common security measures
  - Organisation (assignment of responsibilities)
  - Procedures
  - Physical measures
  - Technical measures

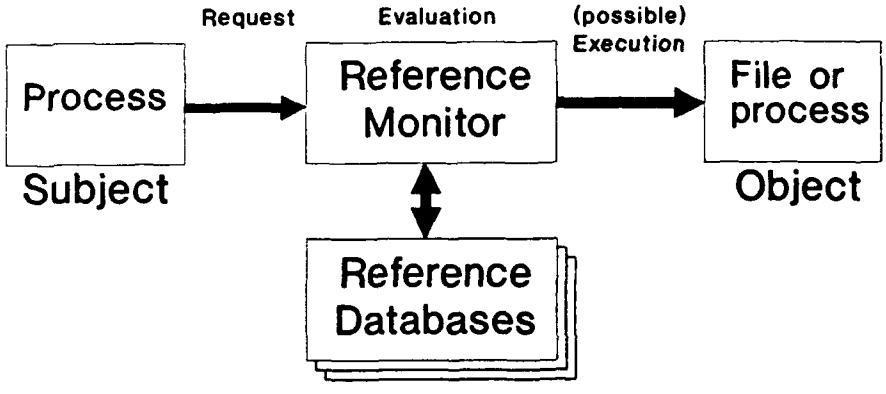
Securicom '91

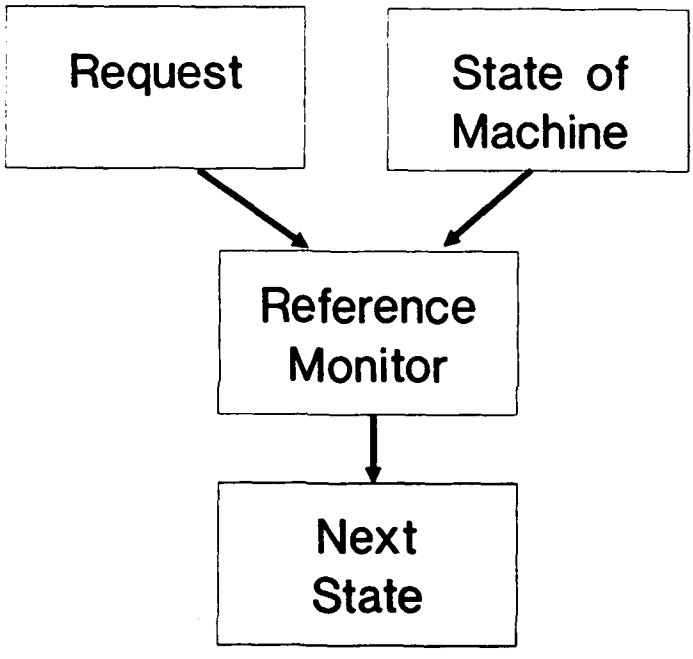
Past
Batch



Past
Interactive, time-sharing



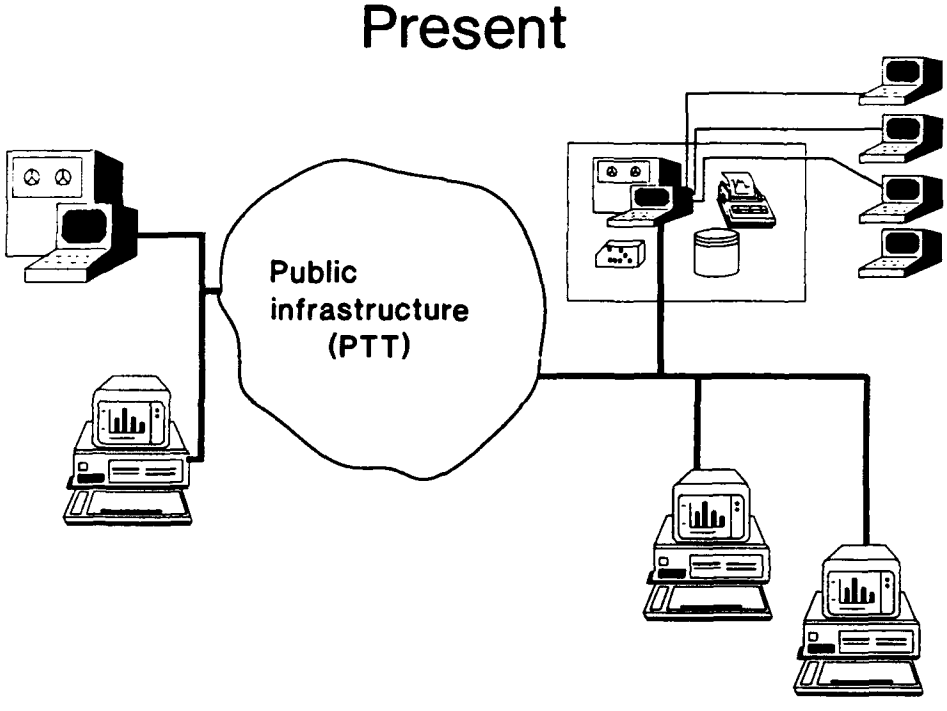

Request
Evaluation
(possible)
Execution
Process
Reference
Monitor
File or
process
Subject
Object
Reference
Databases


Request
State of Machine
Reference Monitor
Next State

Reference Monitor

Main Characteristics:

- Creates Single State Machine
- Mediates all changes within its domain
- Controls its own security information


Present
Public
infrastructure
(PTT)

Present

Characteristics of today

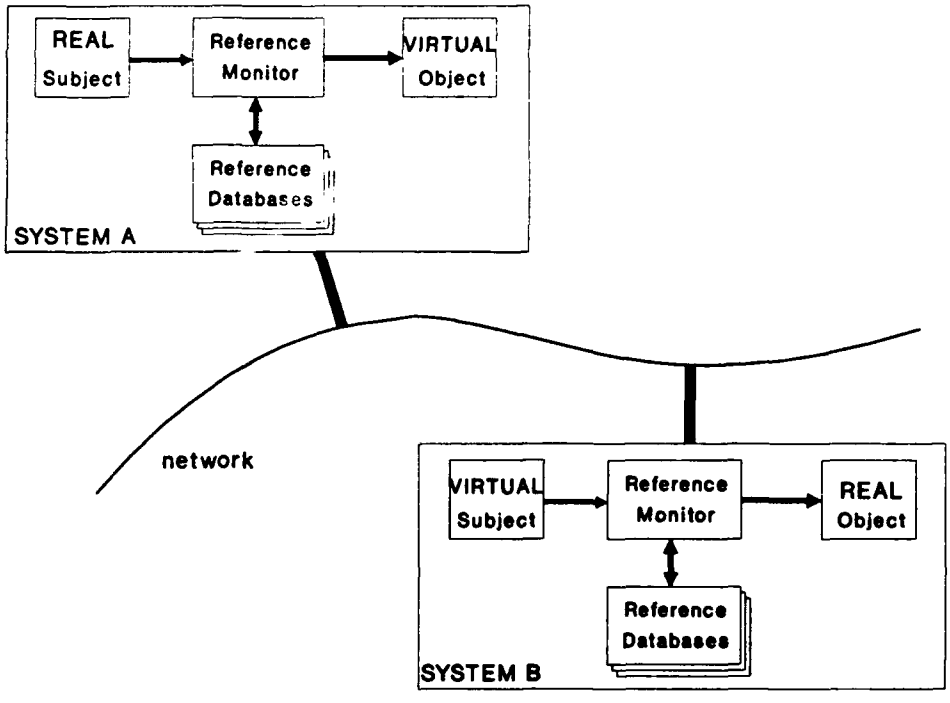
Technical Security

Responsibilities

Security Management

Procedures

Physical Security


REAL
Subject
Reference
Monitor
VIRTUAL
Object
Reference
Databases
SYSTEM A
network
VIRTUAL
Subject
Reference
Monitor
REAL
Object
Reference
Databases
SYSTEM B

Responsibilities

- Who is responsible for security of
  - decentralized systems
  - networks
- Role of central (computer?) department ?

 Shift of responsibilities back to the users

Technical Security Management

- Hardly any tools for integrated management
- Poor integrity mechanisms
- No availability mechanisms

⇨ Security management is not easy

Future
Trends in IT

- Mobile users
  - no fixed working place
  - services and information accessible everywhere
  - dynamic allocation of place of storage
  - processing
  - user does not worry about what is where
- New organisation of services
  - partitioned
  - distributed
  - organised around the network
  - 'hardware' less important

Future

New Security Needs

- Changes in security organisation
- Less impact physical & procedural measures
- Impact of human failures must be diminished

⇨ Technical security must be improved
- integration: applications + O.S. + network
- security is much more than prevention!

Prerequisites for security management:
- standardisation
- general applicable security mechanisms

Summarising

- Development of IT will continue
- New security needs arise
- Security has stayed behind in development

⇨ Trouble ahead?
InfoSec must Anticipate on Changes in IT

- Shifts in responsibilities
- Growing importance of technical security

⇨ Without security, commercial use of new technologies will be very difficult!

UNCLASSIFIED

REPORT DOCUMENTATION PAGE (MOD-NL)

1. DEFENSE REPORT NUMBER (MOD-NL)	2. RECIPIENT'S ACCESSION NUMBER	3. PERFORMING ORGANIZATION REPORT NUMBER
TD91-2007	—	FEL-91-B100

4. PROJECT/TASK/WORK UNIT NO.	5. CONTRACT NUMBER	6. REPORT DATE
20555		MARCH 1991

7. NUMBER OF PAGES	8. NUMBER OF REFERENCES	9. TYPE OF REPORT AND DATES COVERED
43 (INCL. RDP & 1 APPENDIX, EXCL. DISTRIBUTION LIST)	10	FINAL REPORT

10. TITLE AND SUBTITLE
INFORMATION SECURITY: PAST, PRESENT AND FUTURE

11. AUTHOR(S)
P.L. OVERBEEK

12. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
TNO PHYSICS AND ELECTRONICS LABORATORY, P.O. BOX 96864, 2509 JG THE HAGUE
OUDE WAALSDORPERWEG 63, THE HAGUE, THE NETHERLANDS

13. SPONSORING/MONITORING AGENCY NAME(S)

14. SUPPLEMENTARY NOTES

15. ABSTRACT (MAXIMUM 200 WORDS, 1044 POSITIONS)
THE DEVELOPMENT OF INFORMATION SECURITY IS ADRESSED IN RELATION TO THE DEVELOPMENT OF INFORMATION TECHNOLOGY. THE LEADING QUESTION IS: HOW HAS INFORMATION SECURITY DEVELOPED ITSELF SO FAR, AND HOW SHOULD IT PROGRESS TO ADDRESS TOMORROW'S SECURITY NEEDS.
THIS STUDY HAS BEEN PERFORMED AS PART OF THE PHD-PROJECT SEDIS (SECURABLE DISTRIBUTED INFORMATION SYSTEMS). THIS PROJECT AIMS AT A BETTER UNDERSTANDING OF AND CONTRIBUTION TO SECURITY IN DISTRIBUTED INFORMATION SYSTEMS.
THIS PAPER HAS BEEN PRESENTED AT SECURICOM '91, "9e CONGRèS MONDIAL DE LA PROTECTION ET DE LA SéCURITé INFORMATIQUE ET DES COMMUNICATIONS".

16. DESCRIPTORS	IDENTIFIERS
INFORMATION SYSTEMS SECURITY DISTRIBUTED NETWORKS	

17a. SECURITY CLASSIFICATION (OF REPORT)	17b. SECURITY CLASSIFICATION (OF PAGE)	17c. SECURITY CLASSIFICATION (OF ABSTRACT)
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED

18. DISTRIBUTION/AVAILABILITY STATEMENT	17d. SECURITY CLASSIFICATION (OF TITLES)
UNLIMITED	UNCLASSIFIED